AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims

1-23. (Cancelled)

24. (New) An apparatus arranged for receiving a Single Sign-On service request in a telecommunication service network from a user via an access network unable to provide data origin authentication, the user having received access credentials as a result of being authenticated by a core network, the apparatus comprising:

means for receiving the access credentials from the user through the access network;

means for checking validity of the access credentials received from the user;

means for establishing a valid session with the user upon successful validity check of the access credentials;

means for assigning an internal IP address to identify the user in the service network;

means for linking session data, access credentials and assigned internal IP address for the user; and,

means for establishing a secure tunnel with the user when receiving the access credentials through the access network by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunnelled traffic.

25. (New) The apparatus of claim 24, further comprising means for generating service credentials for authorizing the user to access a service in the service network.

26. (New) The apparatus of claim 25, wherein the service credentials are generated on a per service basis for the user upon service request.

27. (New) The apparatus of claim 24, further comprising means for communicating with an Authentication Server of the home network in order to check the validity of the access credentials received from the user when said access credentials are not signed by a recognised authentication entity.

28. (New) The apparatus of claim 24, wherein the means for establishing the secure tunnel with the user are included in a first device named Secure Service Entry Point, and the means for linking session data, access credentials and assigned internal IP address for the user are included in a second device named Single Sign-On Server.

29. (New) The apparatus of claim 28, further comprising means for communicating the Secure Service Entry Point with the Single Sign-On Server.

30. (New) The apparatus of claim 24, further comprising means for an additional co-ordination between the apparatus and an Identity Provider in charge of said user in a home network when said home network is different than the service network which the apparatus is the entry point for.

31. (New) The apparatus of claim 24 for use when the user is accessing a local HTTP service, or an external service in a network different than the currently accessed service network, wherein the apparatus further comprises means for checking whether the user had been previously authenticated or not.

32. (New) The apparatus of claim 31, having means for communicating with an intermediate entity arranged to intercept the user's access to the HTTP local service, or to the external service in an external network.

33. (New) The apparatus of claim 32, wherein the intermediate entity is an HTTP-proxy.

34. (New) The apparatus of claim 32, wherein the intermediate entity is a firewall.

35. (New) The apparatus of claim 24 for use when the user is accessing a non-HTTP local service, further having means for checking whether the user had been previously authenticated or not.

36. (New) The apparatus of claim 24, wherein the means for receiving access credentials comprises means for checking whether a digital certificate issued by the core network is present to indicate a successful authentication of the user.

37. (New) A user equipment arranged to carry out an authentication procedure with a core network, and arranged to access a telecommunication service network via an access network unable to provide data origin authentication, the user equipment, comprising:

means for obtaining access credentials as a result of being authenticated by the core network;

means for sending the access credentials towards the service network when accessing through the access network;

means for establishing a secure tunnel with the service network through the access network, the secure tunnel making use of an outer IP address assigned to the user by the access network for addressing the user;

means for receiving an internal IP address assigned by the service network and included as an inner IP address within the tunnelled traffic to identify the user in the service network; and,

means for linking said access credentials with the inner IP address and with the secure tunnel.

38. (New) The user equipment of claim 37, wherein the means for obtaining access credentials includes:

means for receiving an authentication challenge from the core network;

means for generating and returning an authentication response to the core network;

means for generating a public and private key pair; and,

means for submitting the public key along with a digital signature proving the ownership of the private key towards the core network.

39. (New) The user equipment of claim 37, wherein the means for obtaining access credentials includes:

means for receiving an authentication challenge from the core network;

means for generating and returning an authentication response to the core network; and,

means for requesting a digital certificate obtainable from the core network.

40. (New) The user equipment of claim 39, wherein the means for obtaining access credentials further includes means for generating a public key for which the digital certificate is obtainable.

41. (New) A method for supporting Single Sign-On services in a telecommunication service network for a user accessing said service network through an access network unable to provide data origin authentication, the user having received access credentials as a result of being authenticated by a core network, the method comprising the steps of:

receiving at the service network the access credentials from the user through the access network;

checking validity of the access credentials received at the service network;

establishing a valid session with the user upon successful validity check of the access credentials;

assigning at the service network an internal IP address for the user to identify the user when accessing a service in the service network;

linking session data, access credentials and the assigned internal IP address for the user at an entity of the service network;

establishing a secure tunnel between the user equipment side and an entity of the service network through the access network by using an outer IP address assigned by the access network for addressing the user, and by using as an inner IP address in the tunnelled traffic the internal IP address assigned to identify the user in the service network; and,

linking said access credentials with said inner IP address and with said secure tunnel at the user equipment side.

42. (New) The method of claim 41, further comprising a step of generating service credentials for authorizing the user to access a service in the service network.

43. (New) The method of claim 42, wherein the step of generating service credentials includes a step of generating service credentials on a per service basis for the user upon service request.

44. (New) The method of claim 41, wherein the step of checking the validity of access credentials received from the user at the service network further includes a step of communicating with an Authentication Server of the home network when said access credentials are not signed by a recognised authentication entity.

45. (New) The method of claim 41, wherein the step of linking session data, access credentials and assigned internal IP address for the user further includes a step of communicating a first device named Secure Service Entry Point in charge of the secure tunnel with a second device named Single Sign On Server where the step of linking takes places.

46. (New) The method of claim 41, for use when the user is accessing a local service or an external service in a network different than the currently accessed service network, the method further comprising a step of checking whether the user had been previously authenticated or not.